ABSTRACT

The present invention provides an apparatus configuration for carrying out encryption/decryption securely in an information processing apparatus, communication apparatus or file management apparatus in which information is encrypted/decrypted for security protection.

Since a conventional information processing apparatus comprises a plurality of semiconductor devices, there is a problem that sensitive information may reside on a system bus in the apparatus or a semiconductor memory device serving as main memory therein.

To obviate this problem, the present invention provides the following configuration: In each information processing apparatus, a CPU comprises a microprocessor, a cryptographic processing algorithm ROM, a cryptographic processing hardware circuit, a RAM, a key custody area, and an external bus controller, which are all integrated on a single semiconductor chip. Thus, encryption/decryption processing is carried out only in the CPU, and internal operations of the CPU are made non-analyzable from an external signal of the CPU.